Configurazione del filtro dei contenuti Web con Cisco Umbrella in WAP571 o WAP571E

Obiettivo

L'obiettivo di questo articolo è mostrare come configurare il filtro dei contenuti Web utilizzando Cisco Umbrella su un WAP571 o WAP571E.

Introduzione

Si è lavorato sodo per rendere operativa la rete. Certo, volete che rimanga così, ma gli hacker sono implacabili. Come proteggere la rete Una soluzione consiste nell'impostare il filtro dei contenuti Web. La funzionalità di filtro dei contenuti Web consente di fornire un accesso controllato a Internet mediante la configurazione di criteri e filtri. Consente di proteggere la rete bloccando siti Web dannosi o indesiderati.

Cisco Umbrella è una piattaforma di sicurezza cloud che fornisce la prima linea di difesa dalle minacce su Internet. Funge da gateway tra Internet e i sistemi e i dati per bloccare malware, botnet e phishing su qualsiasi porta, protocollo o applicazione.

Utilizzando un account Cisco Umbrella, l'integrazione intercetterà in modo trasparente (a livello di URL) le query DNS (Domain Name System) e le reindirizzerà a Umbrella. Il dispositivo verrà visualizzato nel dashboard Umbrella come dispositivo di rete per l'applicazione di criteri e la visualizzazione di report.

Per ulteriori informazioni su Cisco Umbrella, consultare i seguenti link:

Cisco Umbrella in breve

Guida per l'utente di Cisco Umbrella

Procedura: Estensione di Cisco Umbrella per la protezione della rete wireless

Dispositivi interessati

WAP571

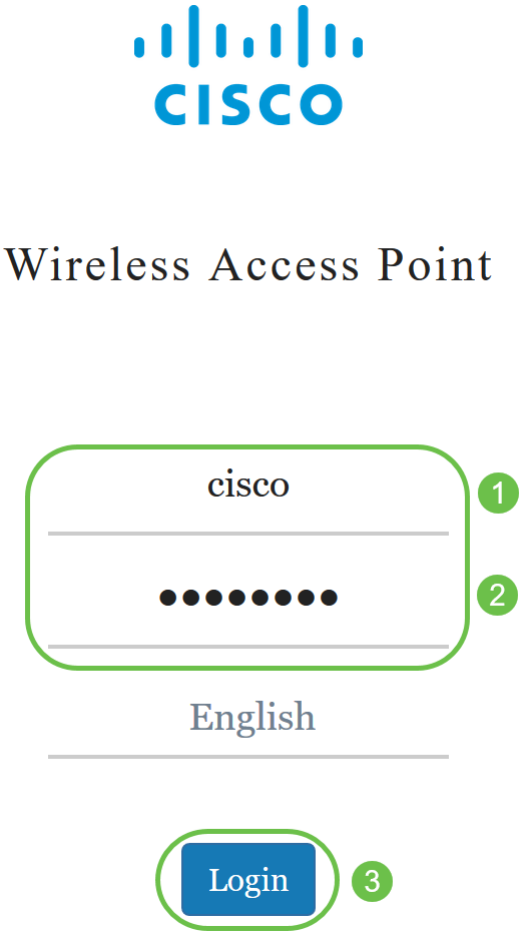
WAP571E

Versione del software

- 1.1.0.3

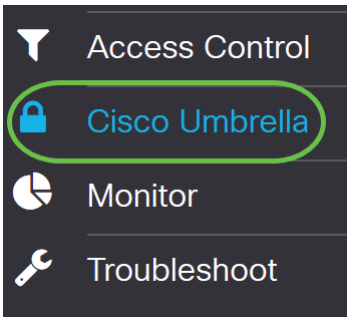
Configurazione di Cisco Umbrella sul WAP

Passaggio 1. Accedere all'utility di configurazione Web di WAP immettendo il nome utente e la password. Il nome utente e la password predefiniti sono cisco/cisco. Se il nome utente o la password sono stati modificati, immettere le nuove credenziali. Fare clic su **Login.**

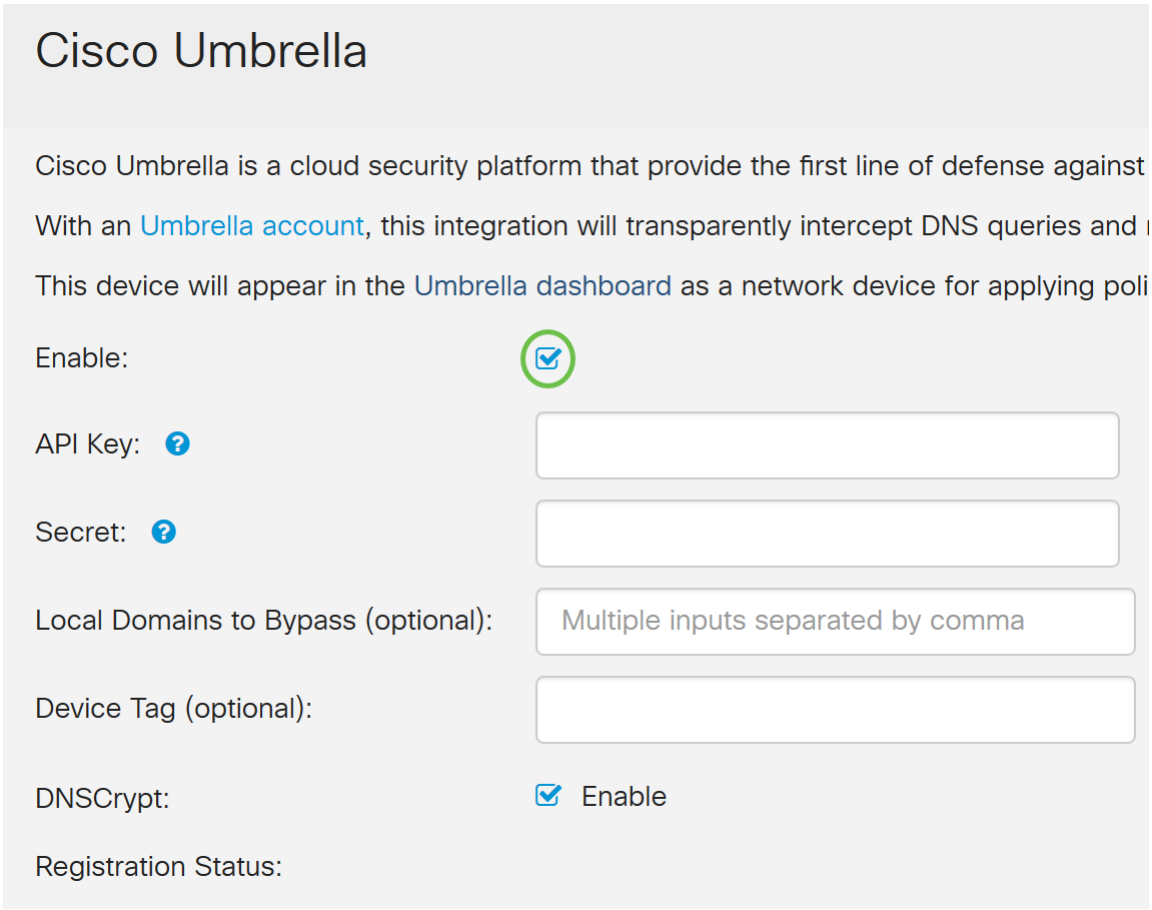


Nota: In questo articolo, il protocollo WAP571E viene usato per dimostrare la configurazione di Cisco Umbrella. Le opzioni del menu possono variare leggermente a seconda del modello del dispositivo.

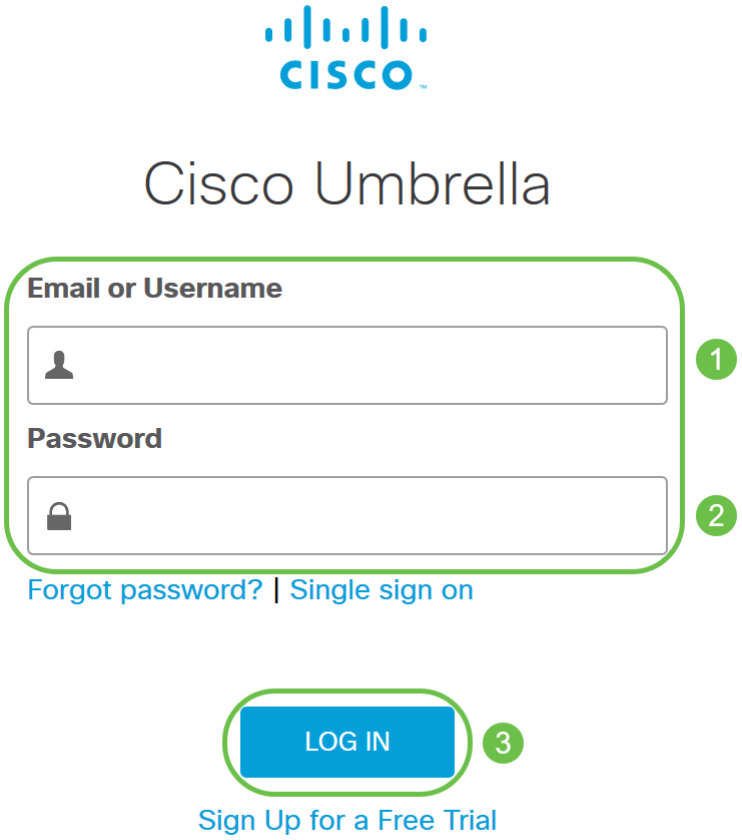
Passaggio 2. Scegliere **Cisco Umbrella**.



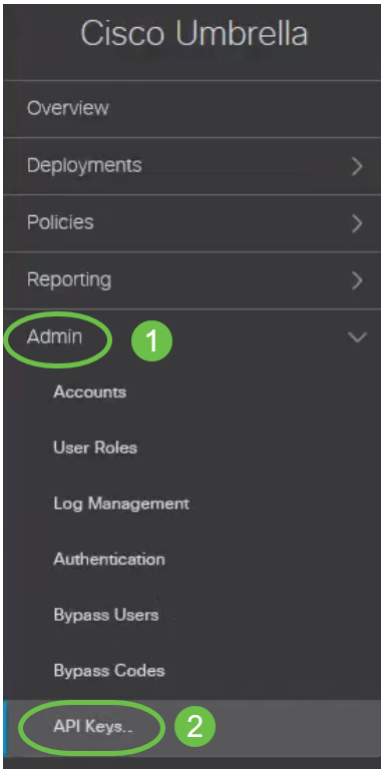
Passaggio 3. *Abilitare* Cisco Umbrella facendo clic sulla casella di controllo.



Passaggio 4. Per ottenere la chiave e il *segreto* API, accedere all'account Cisco Umbrella tramite *e-mail, nome utente* e *password*. Fare clic su **LOG IN**.



Passaggio 5. Passare ad **Admin** e richiedere una chiave API scegliendo **Chiavi API...** dal menu.

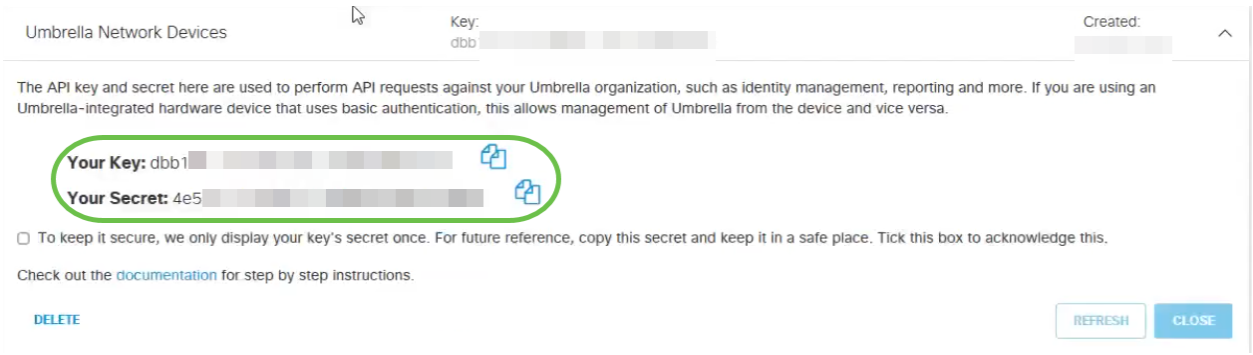


Nota: La prima volta che si richiede una chiave API, viene visualizzata solo la chiave, come mostrato di seguito.

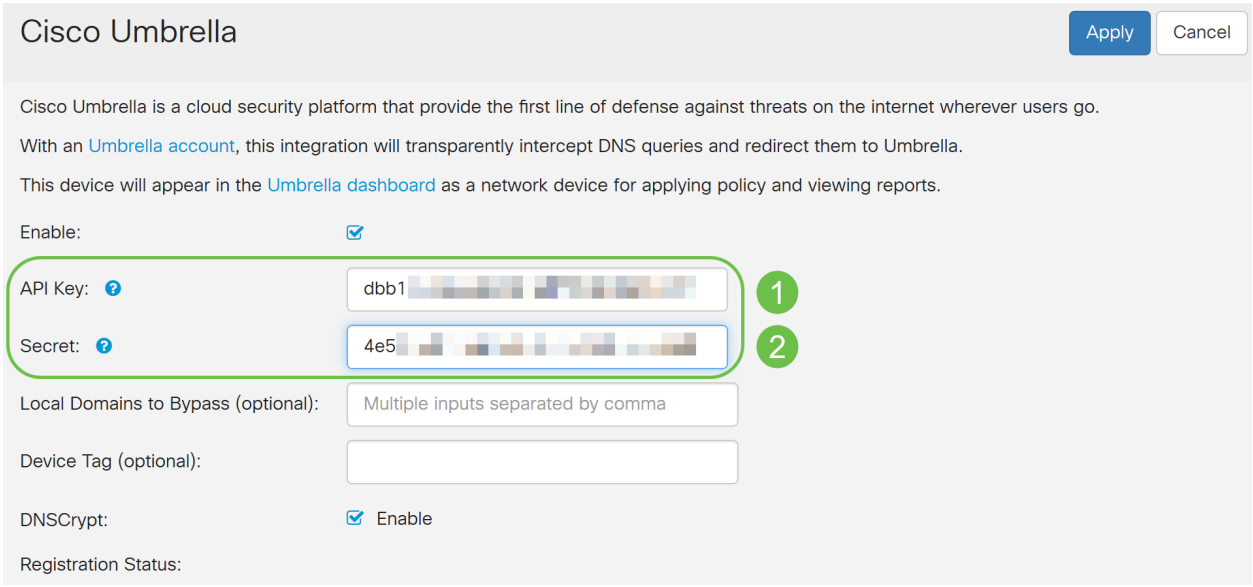
Passaggio 6. Fare clic su **Refresh** per ottenere sia la chiave API che il segreto.

Nota: Quando si fa clic su *Aggiorna*, la chiave API cambia.

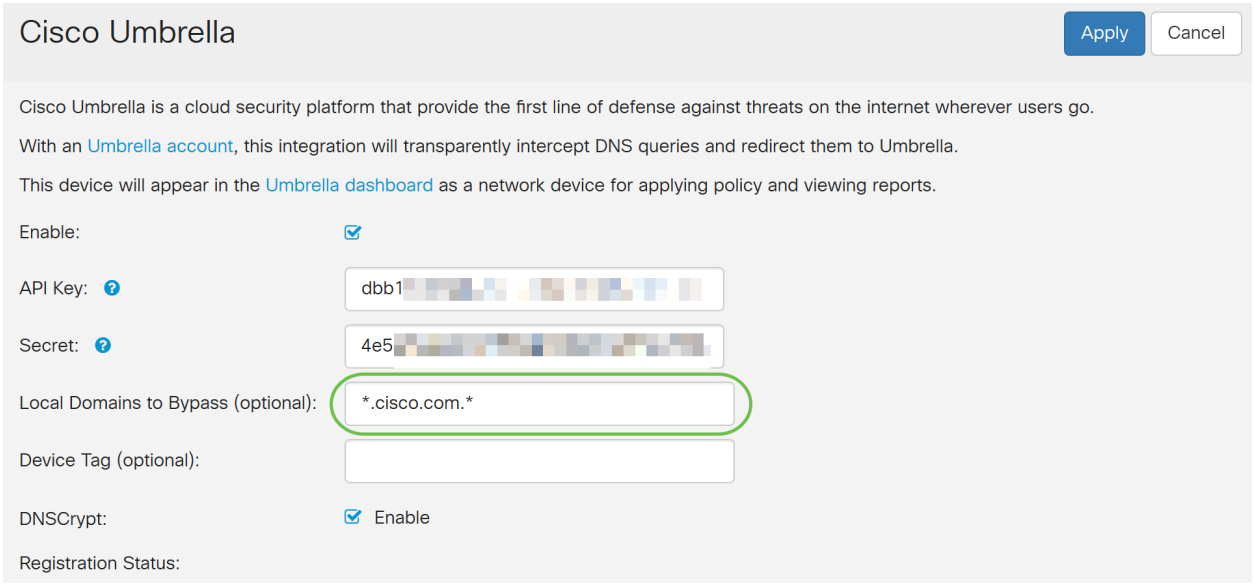
Passaggio 7. Copiare la *chiave* e il *segreto* generati.



Passaggio 8. Incollare la *chiave* e il *segreto* copiati dal passaggio 7 nei campi disponibili nella configurazione *Cisco Umbrella* del WAP.



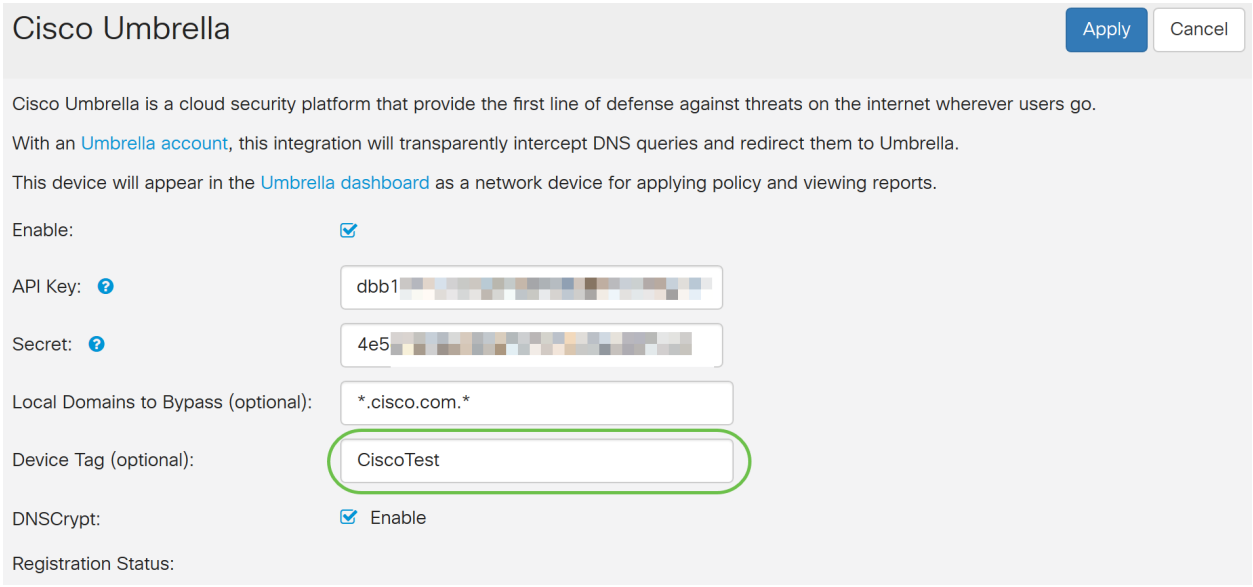
Passaggio 9. (Facoltativo) Immettere il nome di dominio considerato attendibile nel campo **Domini locali da ignorare (facoltativo)** e i pacchetti raggiungeranno la destinazione senza passare per Cisco Umbrella. Gli elementi dell'elenco devono essere separati da una virgola, mentre i domini possono includere caratteri jolly sotto forma di asterisco (*). Ad esempio: *.cisco.com.*



Nota: Questa operazione è necessaria per tutti i domini Intranet e per i domini DNS suddivisi in cui esistono server separati per le reti interne ed esterne.

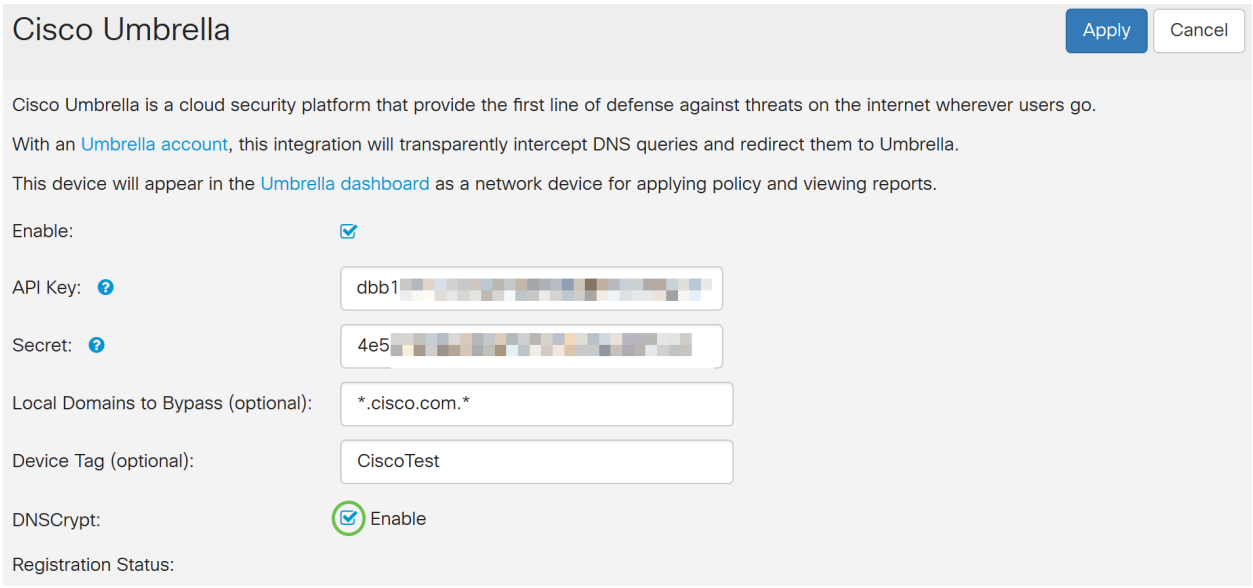
Passaggio 10. (Facoltativo) Immettere un nome di tag nel campo **Tag dispositivo (facoltativo)** per

contrassegnare il dispositivo. Il *codice di matricola* descrive il dispositivo o una particolare origine assegnata al dispositivo. Garantire l'unicità del servizio all'interno dell'organizzazione.

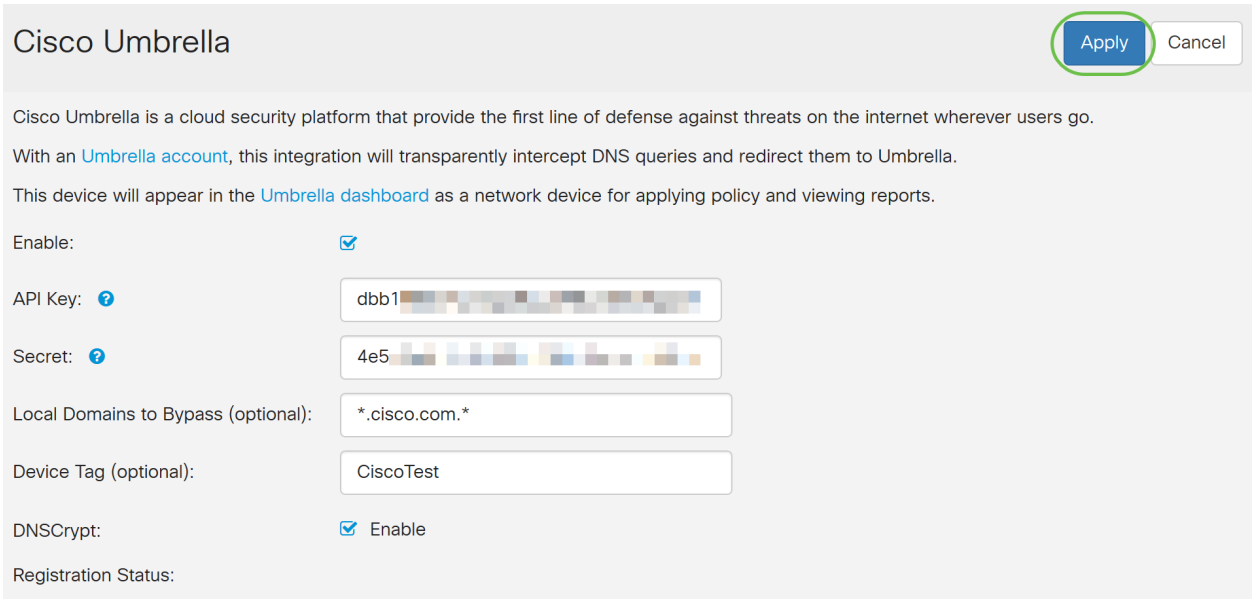


Nota: Qualsiasi modifica apportata ai campi *Secret*, *API Key* e *Device Tag* attiverà una nuova registrazione per creare un dispositivo di rete.

Passaggio 11. **DNSCrypt** viene utilizzato per proteggere (tramite crittografia) la comunicazione DNS tra un client DNS e un resolver DNS. Previene diversi tipi di attacchi DNS e snooping. È attivata per impostazione predefinita.

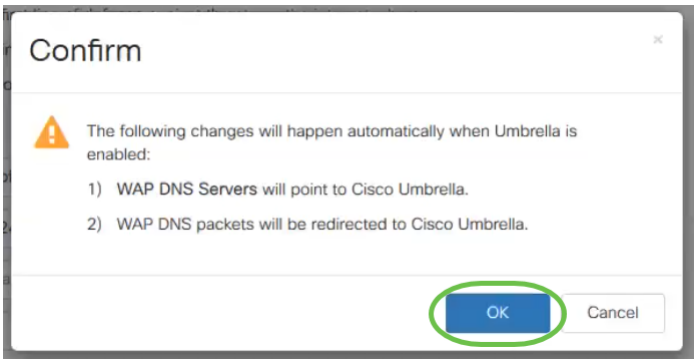


Passaggio 12. Fare clic su **Applica** per applicare queste configurazioni.



Nota: Lo stato della registrazione è indicato nel campo *Stato registrazione*. Lo stato può essere *Riuscito*, *Registrazione* o *Non riuscito*.

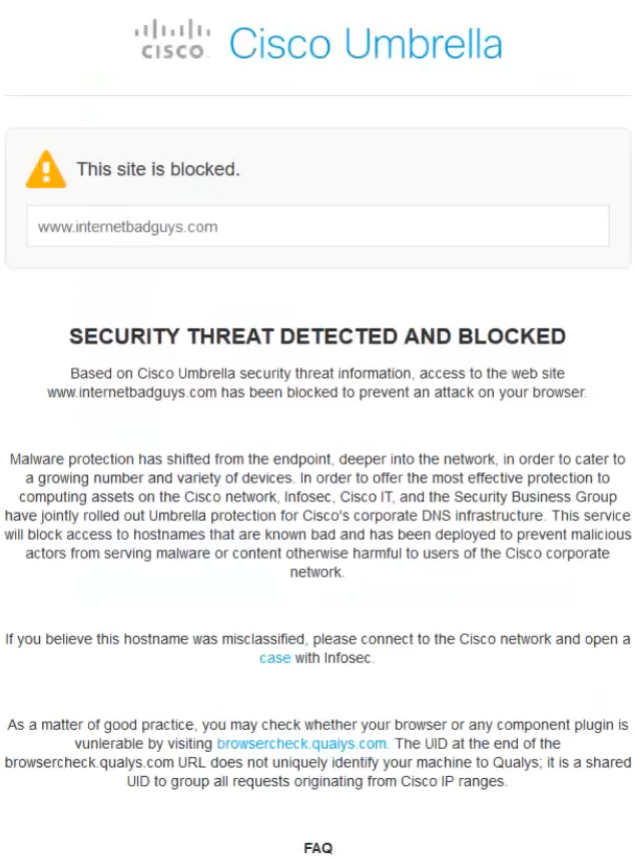
Passaggio 13. Viene visualizzata una schermata di popup come mostrato di seguito. Fare clic su **OK** per confermare.



Verifica

C'è un modo divertente per controllare se il filtro del sito è abilitato. È sufficiente aprire un browser Web e immettere il seguente URL: www.internetbadguys.com. Non abbiate paura, questo è un sito di proprietà di Cisco a scopo di test e verifica.

Poiché il filtro dei siti Web è abilitato in WAP tramite Cisco Umbrella, si riceverà la seguente notifica. La rete wireless reindirizzerà la query DNS a Cisco Umbrella. A sua volta, Cisco Umbrella agisce come server DNS, proteggendo la rete e i suoi utenti.



Conclusioni

Èstato configurato e abilitato il filtro dei siti Web su un access point WAP571 o WAP571E con Cisco Umbrella.

Vuoi saperne di più? Guarda questi video relativi a Cisco Umbrella:

Cisco Tech Talk: Protezione di una rete aziendale tramite i punti di accesso per piccole imprese Umbrella e Cisco

Cisco Tech Talk: Come ottenere un account Umbrella

Cisco Tech Talk: Impostazione di un criterio Umbrella